The Habits of Highly Successful Security Awareness Programs

Samantha Manke, Security Analyst
Governance Risk and Compliance - G12

WHY SECURITY AWARENESS?

Why Security Awareness?

- The human factor
  - Technology can only help so much
- Security Awareness programs are in integral part of a mature security program
- Cost-Effective Solution
- Required by standards and regulations

The Problem with Security Awareness Programs

- Varying degrees of quality in awareness programs
- The 3-year cycle
- Poor security cultures

THE STUDY: OPPORTUNITY STATEMENT AND METHODOLOGY

Opportunity Statement

- My work experience allowed me the unique experience to build a program from scratch
- The local ISSA chapter's Security Awareness user group (a.k.a. "Support Group") meets bi-monthly and delegates were willing participants
- Security Awareness material is seen as non-proprietary

Approach/Methodology

- Qualitative
  - Face-to-face interviews with Security Awareness Specialists
- Quantitative
    - 2 Surveys
      - 1 for Security employees
      - 1 for Non-Security employees
- Limitations

STUDY: ANALYSIS

Analysis-General Trends

- In the end a total of 7 companies participated
  - 2 from the Health Sector
  - 2 from the Manufacturing Sector
  - 1 from the Food Sector
  - 1 from the Financial Sector
  - 1 from the Retail Sector
- Companies were often surprisingly honest about the success of their programs
- No participating company had any metrics to assess their effectiveness

Analysis-General Trends

- Most companies struggle to gain support:
  - From upper management
  - From key departments
  - From their user population
- Compliance:
  - PCI helps with support and budget
  - HIPAA does not
- Variety of approaches
  - Some Security Awareness Specialists had a security background while others had a marketing or communications background
  - Companies had 1-26 employees contributing to efforts

Analysis-Security Respondents

- 87% of Security Respondents (“SRs”) reported their programs are successful
- Roughly half reported having difficulty encouraging their employees to take security seriously
- Only 19% reported a lack of support from management

Analysis-Security Respondents

- 26% reported a lack of enthusiasm for their efforts
- 50% reported having difficulty receiving funding for their initiatives

Analysis-Non-Security Respondents

- 100% of Non-Security employees reported having learned something from their company's Security Awareness program
- 100% reported being "security-minded individuals"
- 100% reported thinking their company's Security Awareness programs are successful

Analysis: Non-Security Respondents

- Only 60% reported changing their behavior as a result of Security Awareness
- 92% reported viewing their Security team positively
- 12% reported having conflicts with their Security team

Results

- **Security is difficult to administer at most companies**
- **Compliance helps with enforcement and awareness**
- **Creativity and/or mandatory training are the key(s) to success**
- **Companies with more top-level support are more successful**

STUDY: RECOMMENDATIONS

Where to Start?

- Build on Existing Program or Start Over?
- How developed is your current program?
- Would starting anew breath fresh life into it?

Create a Strong Foundation

- This is the main source of failure
- Make a 3-month plan
- Topics may change

Assess Approach

- Softball
- Hard push
- Avoid fear-mongering

Organizational Buy-in

- Appeal to the highest level you are able to engage
- Market some materials to the C-level
- Stress benefits of Security Awareness

Deciding which components your program should have

- Which mediums of communication will be most effective at your company?
- Which mediums are already saturated?
- What are employees most receptive to?

Recommended components

- Website
- Posters
- Newsletters/Blog
- Monthly tips
- Lunch and Learns
- Roadshows
- Speakers
- Security Week

More Creative Endeavors

- Guerilla marketing campaign
- Security Cube
- Demonstrations and movie showings

Gather Metrics

- No participating company gathered metrics
- Compare rate of reported incidents pre and post
  - Collecting metrics ahead of time so you can potentially measure success after the fact
  - Should you do a pen test/assessment?

Assessing Success

- Assess which components have been successful
- Administer a survey
  - Try to keep it anonymous
  - Offer a drawing that employees can enter for a prize
- Understand limitations

Keep program fresh

- Easy to fall behind
- Pay attention to the news
- Create new material for every month

CONCLUSIONS

Conclusions

- **Focus on building support before spending too much time on other aspects**
- **Do a thorough assessment of culture before starting or revamping program**
- **Security is dysfunctional at most companies**

Next steps

- ISSA's "Great Security Awareness Experiment" series
- Many opportunities for additional research
  - Non-security employees should be re-surveyed
  - Additional companies from different sectors could be included
  - A deeper dive into participating companies could be conducted to ask about discrepancies

For more information:

- Samantha.E.Manke@Gmail.com
- +1-651-325-5902
- http://www.linkedin.com/pub/samantha-manke/21/34/779